

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
EASTERN DIVISION
No. 5:19-cv-00475-BO

JASON WILLIAMS,)
)
Plaintiff,)
)
v.)
)
AT&T MOBILITY, LLC,)
)
Defendants)

**PLAINTIFF JASON WILLIAMS'S OPPOSITION TO DEFENDANT
AT&T MOBILITY LLC'S MOTION TO DISMISS COMPLAINT**

**PIERCE BAINBRIDGE BECK
PRICE & HECHT LLP**

Christopher LaVigne
clavigne@piercebainbridge.com
Sarah Baugh
sbaugh@piercebainbridge.com
277 Park Avenue, 45th Floor
New York, NY 100172
Telephone: (212) 484-9866
Facsimile: (646) 968-4125

Counsel for Plaintiff Jason Williams

**PIERCE BAINBRIDGE BECK
PRICE & HECHT LLP**

Dwayne D. Sam
dsam@piercebainbridge.com
601 Pennsylvania Avenue NW
South Tower, Suite 700
Washington, DC 20004
Telephone: (202) 843-8342
Facsimile: (202) 899-5666

SHUMAKER LOOP & KENDRICK LLP

Terence S. Reynolds
treynolds@shumaker.com
Lucas D. Garber
lgarber@shumaker.com
101 South Tyron Street
Suite 2200
Charlotte, North Carolina 28280

*Local Civil Rule 83.1(d) Counsel for Plaintiff
Jason Williams*

TABLE OF CONTENTS

| | | |
|------|--|----|
| I. | INTRODUCTION | 1 |
| II. | ARGUMENT | 2 |
| | A. Standard of Review | 2 |
| | B. Mr. Williams Adequately Alleged Proximate Cause..... | 3 |
| | 1. Mr. Williams Adequately Alleged How the Illegal SIM Swaps Caused the Loss of \$2 million. | 3 |
| | 2. Mr. Williams’ claims are not based on unforeseeable, independent criminal acts. | 6 |
| | C. Mr. Williams Has Established Article III Standing. | 10 |
| | D. Mr. Williams Is Entitled to Damages and Injunctive Relief under the Federal Communications Act. | 11 |
| | E. Mr. Williams Alleges Reliance Under the North Carolina Unfair and Deceptive Trade Practices Act..... | 13 |
| | F. Mr. Williams’ Claims Are Not Barred By the Economic Loss Doctrine | 17 |
| | 1. Mr. Williams Sustained Injury Outside the Scope of the Privacy Policy | 18 |
| | 2. AT&T is Charged by Law to Protect Mr. Williams’ CPNI..... | 18 |
| | G. None of the Exceptions to the North Carolina Anti-Hacking Statute Apply Here..... | 21 |
| | H. Mr. Williams’ CFAA Claim is Adequately Pled..... | 23 |
| | I. Mr. Williams’ Prayer for Punitive Damages Should Not Be Stricken | 25 |
| III. | CONCLUSION..... | 28 |

TABLE OF AUTHORITIES

| | Page(s) |
|---|---------|
| Cases | |
| <i>Anita's N.M. Style Mexican Food, Inc. v. Anita's Mexican Foods Corp.</i> , 201 F.3d 314 (4th Cir. 2000) | 2 |
| <i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009)..... | 2 |
| <i>Bechhoefer v. Dep't of Justice</i> , 209 F.3d 57 (2d Cir. 2000), <i>aff'd</i> , 312 F.3d 563 (2d Cir. 2002) | 12 |
| <i>Bell Atl. v. Twombly</i> , 550 U.S. 544 (2007)..... | 1, 2, 5 |
| <i>In re Brokers, Inc.</i> , 407 B.R. 693 (Bankr. M.D.N.C. 2009)..... | 6 |
| <i>Bussian v. DaimlerChrysler Corp.</i> , 411 F. Supp. 2d 614 (M.D.N.C. 2006) | 15 |
| <i>CBP Res., Inc. v. SGS Control Servs., Inc.</i> , 394 F. Supp. 2d 733 (M.D.N.C. 2005) | 15 |
| <i>Cent. Wesleyan Coll. v. W.R. Grace & Co.</i> , 6 F.3d 177 (4th Cir. 1993) | 25 |
| <i>In re Comm'cns Satellite Corp.</i> , 97 F.C.C.2d 82 (1984) | 11 |
| <i>Conboy v. AT&T Corp.</i> , 241 F.3d 242 (2d Cir. 2001)..... | 11 |
| <i>Davenport v. D.M. Rental Props., Inc.</i> , 718 S.E.2d 188 (N.C. Ct. App. 2011) | 9, 10 |
| <i>Devine v. United States</i> , 202 F.3d 547 (2d Cir. 2000)..... | 12 |
| <i>Everhart v. O'Charley's Inc.</i> , 683 S.E.2d 728 (N.C. Ct. App. 2009) | 26, 27 |
| <i>FTC v. Affiliate Strategies, Inc.</i> , 2010 WL 11470099 (D. Kan. June 4, 2010)..... | 15 |

| | |
|---|--------|
| <i>Hatteras/Cabo Yachts, LLC v. M/Y EPIC</i> , 2019 WL 5792863 (E.D.N.C. Nov. 6, 2019)..... | 19 |
| <i>Hedrick v. S. States Coop. Inc.</i> , 2010 WL 3834631 (E.D.N.C. Sept. 30, 2010)..... | 2 |
| <i>Holt v. N.C. Dep't of Transp.</i> , 781 S.E.2d 697 (N.C. Ct. App. 2016), <i>aff'd</i> , 369 N.C. 57 (2016) | 6 |
| <i>Int'l Telecomm. Exchange Corp. v. MCI Telecomm. Corp.</i> , 892 F. Supp. 1520 (N.D. Ga. 1995)..... | 11 |
| <i>Johnson v. Dep't of Treasury</i> , 700 F.2d 971 (5th Cir. 1983), <i>abrogated by Doe v. Chao</i> , 124 S. Ct. 1204 (2004)..... | 12, 13 |
| <i>Kelly v. Ga.–Pac. LLC</i> , 671 F. Supp. 2d 785 (E.D.N.C. 2009)..... | 17 |
| <i>Legacy Data Access, Inc. v. Cadrillion, LLC</i> , 889 F.3d 158 (4th Cir. 2018) | 19 |
| <i>Madison River Mgmt. Co. v. Bus. Mgmt. Software Corp.</i> , 351 F. Supp. 2d 436 (M.D.N.C. 2005) | 16 |
| <i>Martin v. Smith</i> , 534 F. Supp. 804 (W.D.N.C. 1982) | 3 |
| <i>Appeal of Martin</i> , 209 S.E.2d 766 (N.C. 1974)..... | 21 |
| <i>Matthews v. Consol. Grp. Claims, Inc.</i> , 1998 WL 1037919 (M.D.N.C. Dec. 18, 1998) | 2 |
| <i>McCauley v. Home Loan Inv. Bank, F.S.B.</i> , 710 F.3d 551 (4th Cir. 2013) | 16, 17 |
| <i>N.C. State Ports Auth. v. Lloyd A. Fry Roofing Co.</i> , 240 S.E.2d 345 (N.C. 1978), <i>rejected by Trs. Of Rowan Tech. Coll. v. J. Hyatt Hammond Assocs., Inc.</i> , 313 N.D.C 230 (1985)..... | 17, 19 |
| <i>Nat'l Fin. Partners Corp. v. Ray</i> , 2014 WL 5148197 (Sup. Ct. Union Cnty. Oct. 13, 2014) | 11 |
| <i>U.S. ex rel. Nathan v. Takeda Pharms. N. Am., Inc.</i> , 707 F.3d 451 (4th Cir. 2013) | 16 |

| | |
|--|----|
| <i>In re New Bern Riverfront Dev., LLC</i> , 2011 WL 5902621 (Bankr. E.D.N.C. May 24, 2011)..... | 19 |
| <i>Newton v. Standard Fire Ins. Co.</i> , 291 N.C. 105 (1976) | 25 |
| <i>Sageworks, Inc. v. Creatore</i> , 2017 WL 633359 (E.D.N.C. Feb. 15, 2017)..... | 24 |
| <i>Sansotta v. Town of Nags Head</i> , 97 F. Supp. 3d 713 (E.D.N.C. 2014)..... | 3 |
| <i>Sea Side Villas II Horizontal Prop. Regime v. Single Source Roofing, Corp.</i> , 64 F. App'x 367 (4th Cir. 2003) | 19 |
| <i>Sec. Credit Corp. v. Mid/East Acceptance Corp. of N.C., Inc.</i> , 2012 WL 1337400 (N.C. Ct. App. Apr. 17, 2012) | 25 |
| <i>Spokeo, Inc. v. Robins</i> , 136 S. Ct. 1540 (2016)..... | 10 |
| <i>State v. Taylor</i> , 572 S.E.2d 237 (N.C. Ct. App. 2002) | 3 |
| <i>Tech. Partners, Inc. v. Papaioannou</i> , 2015 WL 9304562 (W.D.N.C. Dec. 21, 2015) | 24 |
| <i>Tech Sys., Inc. v. Pyles</i> , 630 F. App'x 184 (4th Cir. 2015) | 24 |
| <i>Ticketmaster L.L.C. v. Prestige Entm't W., Inc.</i> , 315 F. Supp. 3d 1147 (C.D. Cal. 2018) | 23 |
| <i>Time, Inc. v. Hill</i> , 385 U.S. 374 (1967)..... | 13 |
| <i>A.V. ex rel. Vanderhye v. iParadigms, LLC</i> , 562 F.3d 630 (4th Cir. 2009) | 24 |
| <i>Vess v. Ciba–Geigy Corp. USA</i> , 317 F.3d 1097 (9th Cir. 2003) | 2 |
| <i>W. Cap. Partners, LLC v. Brookhollow, LLC</i> , 2007 WL 1202851 (E.D. Va. Apr. 19, 2007) | 11 |
| <i>WEC Carolina Energy Sols. LLC v. Miller</i> , 687 F.3d 199 (4th Cir. 2012) | 25 |

| | |
|--|---|
| <i>Westfarm Assocs. Ltd. P'ship v. Wash. Suburban Sanitary Comm'n</i> , 66 F.3d 669 (4th Cir. 1995) | 6 |
|--|---|

| | |
|--|----|
| <i>Wilkins v. Denamerica Corp.</i> , 2001 WL 1019698 (W.D.N.C. May 5, 2001) | 26 |
|--|----|

Federal Statutes

| | |
|------------------------|---------------|
| 5 U.S.C. § 552 | 13 |
| 18 U.S.C. § 1030 | 23, 25 |
| 28 U.S.C. § 1331 | 11 |
| 28 U.S.C. § 1367 | 11 |
| 47 U.S.C. § 222 | <i>passim</i> |

North Carolina Statutes

| | |
|----------------------------------|--------|
| N.C.G.S.A. § 1D-15 | 26 |
| N.C. Gen. Stat. § 14-453.1 | 21, 22 |
| N.C. Gen. Stat. § 1-539.2A | 21, 23 |
| N.C. Gen. Stat. § 14-458 | 22 |

Federal Rules

| | |
|--------------------------------|------------|
| Fed. R. Civ. P. 8 | 1 |
| Fed. R. Civ. P. 9 | 15, 16, 17 |
| Fed. R. Civ. P. 12(b)(6) | 1, 2, 16 |
| Fed. R. Civ. P. 15 | 2 |

Other Authorities

| | |
|--|----|
| Brian Rexroad, “ <i>Secure Your Number to Reduce SIM Swap Scams</i> ,” AT&T’s Cyber Aware (Sept. 2017), available at https://about.att.com/pages/cyberaware/ni/blog/sim_swap | 27 |
|--|----|

I. INTRODUCTION

A team of criminals working for and with AT&T executed multiple unauthorized and illegal SIM swaps of Jason Williams' phone, and then used their newfound access to reset the passwords to Mr. Williams' digital, financial accounts and ultimately steal his property. Unable to deny its involvement in these criminal acts, AT&T marshals a host of red herring, whataboutism inquiries to make it appear as though the theft of Mr. Williams' property was utterly unforeseeable and unrelated to the SIM swaps. But AT&T knows, and the Complaint clearly states, exactly *how* the theft occurred and *who* was involved in carrying out this brazen heist. The Court should therefore reject AT&T's stratagem as it seeks to obfuscate what the Complaint makes clear: AT&T knew, or should have known, that its portable SIM cards were an attack vector that was actively being exploited before the events at issue here, and AT&T failed to take adequate steps to prevent the situation.

At its core, the pending motion to dismiss Mr. Williams' Complaint rests on a fundamental distortion of the pleading standards under Rules 8 and 12(b)(6) of the Federal Rules of Civil Procedure. AT&T not only asks the Court to disregard Mr. Williams' well-pled factual allegations, but it also seeks to impose on him a "heightened fact pleading of specifics" which is contrary to the plausibility standard. *See Bell Atl. v. Twombly*, 550 U.S. 544, 570 (2007) ("we do not require heightened fact pleading of specifics, but only enough facts to state a claim to relief that is plausible on its face"). To the extent AT&T has true inquiries about what happened, the parties should proceed to discovery.

In the face of detailed allegations relating to how AT&T's conduct in Mr. Williams' SIM swaps resulted in significant damages, AT&T improperly insists upon a level of detail relating to proximate cause that is contrary to anything required at the pleading stage.

Equally improper, AT&T disregards its obligations to accept as true the facts alleged in the Complaint and the reasonable inferences therefrom, and instead engages in a highly selective reading of the allegations in the Complaint.

AT&T's motion to dismiss should be denied.

II. ARGUMENT

A. Standard of Review

A motion to dismiss under Rule 12(b)(6) challenges the legal sufficiency of the claims stated in the Complaint. *See* Fed. R. Civ. P. 12(b)(6). To survive a motion to dismiss, the plaintiff's complaint "must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544 (2007)). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* A complaint that offers mere "labels and conclusions" or "a formulaic recitation of the elements of a cause of action will not do." *Id.* (citation omitted). In deciding a Rule 12(b)(6) motion, the Court must consider all facts alleged in the complaint as true and construe the allegations in the light most favorable to the pleader. *Anita's N.M. Style Mexican Food, Inc. v. Anita's Mexican Foods Corp.*, 201 F.3d 314, 316 (4th Cir. 2000).

The court should freely grant a plaintiff leave to amend a deficient claim "when justice so requires." Fed. R. Civ. P. 15(a)(2). Absent any indication of prejudice, undue delay or bad faith, leave to amend should be granted where the plaintiff may cure the alleged deficiencies in its original complaint. *Matthews v. Consol. Grp. Claims, Inc.*, 1998 WL 1037919, at *2 (M.D.N.C. Dec. 18, 1998); *Hedrick v. S. States Coop. Inc.*, 2010 WL 3834631, at *3 (E.D.N.C. Sept. 30, 2010); *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1108 (9th Cir. 2003) ("[L]eave to amend

should be granted if it appears at all possible that the plaintiff can correct the defect.”) (citation omitted).

B. Mr. Williams Adequately Alleged Proximate Cause.

Generally, proximate cause is a question of fact for the jury. *Sansotta v. Town of Nags Head*, 97 F. Supp. 3d 713, 735 (E.D.N.C. 2014); *Martin v. Smith*, 534 F. Supp. 804, 806 (W.D.N.C. 1982) (“Under accepted North Carolina law, the proximate cause of an injury is a factual question for the jury, rather than a question of law for the court.”). Here, Mr. Williams has provided enough facts to adequately plead that AT&T’s acts or omissions were the proximate cause of his loss of over \$2 million and other damages, and any questions surrounding it are factual and inappropriate for resolution at this stage.

1. Mr. Williams Adequately Alleged How the Illegal SIM Swaps Caused the Loss of \$2 million.

AT&T wrongfully characterizes Mr. Williams’ detailed claims against it as “conclusory statements” that have “no factual allegations to connect AT&T[]” to Mr. Williams’ losses. Mot. at 7. AT&T also goes so far as to blame Mr. Williams for his damages; indeed, AT&T faults Mr. Williams’ “own negligence in failing to better protect his own private information” as the reason he suffered financial loss, death threats, and his and his family’s private information being disseminated to dangerous criminals.¹ *Id.* at 7–8.

¹ AT&T does not indicate how Mr. Williams was contributorily negligent, except by noting it that it was negligent to store private information within his email account and that he should have used other password protection tools. This statement borders on ludicrous as AT&T itself has noted how commonplace it is for private information to be store within email accounts. *See* Compl. ¶ 134. But even if Mr. Williams were contributorily negligent (and he is not), that would not diminish AT&T’s liability. *See State v. Taylor*, 572 S.E.2d 237, 241 (N.C. Ct. App. 2002) (“Contributory negligence on the part of a victim does not preclude the jury’s consideration of a defendant’s culpable conduct. The jury is responsible for determining if a defendant’s culpable conduct is a proximate cause of the victim’s injury and must decide guilt or innocence on that

AT&T further claims “there are no allegations explaining how control of Mr. Williams’ wireless telephone number . . . enabled the hackers to access [[his] bank, cloud storage, cryptocurrency, email, and social media accounts.” *Id.* at 7. This is incorrect, and to make that assertion, AT&T ignores entire pages of the Complaint detailing how a SIM swap is much more than a mere transfer of a phone number. *See* Compl. ¶¶ 22–29, 36–46.

Here, Mr. Williams has provided enough facts to adequately plead that AT&T’s acts or omissions were the proximate cause of his loss of almost \$2 million. In the Complaint, Mr. Williams explained that SIM swapping transfers control over a phone number, which includes not only texting and phone capabilities, but password reset capabilities. *Id.* ¶¶ 26–27. Mr. Williams explained that when an unauthorized SIM swap occurs, this moves the victim’s phone service, and incoming data, texts, and calls to a phone controlled by the hacker. *Id.* ¶ 26.

This allows the hacker to exploit the two-factor authentication process, and either access the victim’s accounts without a password, or reset the password by having a reset code sent to the hacked phone via text messaging. *Id.* ¶¶ 22–29. AT&T cannot feign ignorance regarding the capabilities SIM swapping provides hackers, as the company itself has admitted that “SIM swapping . . . [provides] control over victims’ phone numbers” and that phones are “mini-computers” that contain “so much personal data”, “[our] life” and virtually “everything” about a person. *Id.* ¶¶ 131, 135. AT&T has also noted that “most people do have something valuable [in their email accounts], which is access to all their other accounts, which you can get with a password reset.” *Id.* ¶ 134. In claiming that there are no allegations that a SIM swap enabled hackers to steal

basis. [] Consideration of this proximate causation is not contingent upon a showing that the victim was not contributorily negligent.”).

from Mr. Williams, AT&T illogically refuses to acknowledge that a SIM swap effectively transfers the key to the victim's digital life—email, online banking, social media, etc.

Further, by arguing that Mr. Williams failed to allege facts showing that a SIM swap led to Mr. Williams' losses, AT&T ignores the well-pled allegations in the Complaint explaining how gaining control over a phone number is essentially gaining control over many digital accounts through two-factor authentication. As alleged in the Complaint, a 2017 report by the U.S. Fair Trade Commission stated in relevant part:

Having a mobile phone account hijacked can waste hours of a victim's time and cause them to miss important calls and messages. However, this crime is particularly problematic due to the growing use of text messages to mobile phones as part of authentication schemes for financial services and other accounts. The security of two-factor authentication schemes that use phones as one of the factors relies on the assumption that someone who steals your password has not also stolen our phone number. Thus, mobile carriers and third-party retailers need to be vigilant in their authentication practices to avoid putting their customers at risk of major financial loss and having email, social network, and other accounts compromised.

Compl. ¶ 126.

At bottom, AT&T knew or should have known that a stolen phone can be as effective as a stolen password. It is simply not believable that AT&T is ignorant of these basic facts. If AT&T argues otherwise, following discovery, it is for a jury to determine.

Under *Twombly*, this Court does not need specifics on how exactly hackers accessed Mr. Williams' financial accounts. *Twombly* requires “only enough facts to state a claim to relief that is plausible on its face.” 550 U.S. at 570. And, as noted by North Carolina courts, proximate cause is a factual issue. Mr. Williams has alleged enough facts to state a plausible claim for relief, and any dispute about what happened is factual in nature and not appropriate to be dismissed at this stage.

2. Mr. Williams' claims are not based on unforeseeable, independent criminal acts.

AT&T incorrectly argues that it cannot be held liable because criminal acts of a third party contributed to Mr. Williams' loss. Mot. at 8. Contrary to AT&T's contention, even without a "special relationship", "[p]roximate cause may be found even where the **conduct of the third party is tortious or criminal**, so long as the conduct was facilitated by the first party and reasonably foreseeable, and some ultimate harm was reasonably foreseeable." *Westfarm Assocs. Ltd. P'ship v. Wash. Suburban Sanitary Comm'n*, 66 F.3d 669, 688 (4th Cir. 1995) (emphasis added); *In re Brokers, Inc.*, 407 B.R. 693, 722 (Bankr. M.D.N.C. 2009) ("[n]evertheless, if there is evidence that the criminal acts that occurred were reasonably foreseeable, the negligent actor may be held liable.").

Under North Carolina law, "[i]t is immaterial how many new events or forces have been introduced if the original cause remains operative and in force. In order for the conduct of the intervening agent to break the sequence of events and stay the operative force of the negligence of the original wrongdoer, the intervening conduct must be of such nature and kind that the **original wrongdoer had no reasonable ground to anticipate it**." *Holt v. N.C. Dep't of Transp.*, 781 S.E.2d 697, 704 (N.C. Ct. App. 2016), *aff'd*, 369 N.C. 57 (2016) (emphasis added).

"The new, independent, intervening cause must **be one not produced by the wrongful act or omission**, but independent of it, and adequate to bring about the injurious result; a cause which interrupts the natural sequence of events, turns aside their course, prevents the natural and probable result of the original act or omission, and produces a different result, that reasonably might not have been anticipated." *Id.* at 704 (emphasis added). "The connection [between the negligence and the damages] is not actually broken if the intervening event is one which might in the natural

and ordinary course of things, be anticipated *as not entirely improbable*, and the defendant’s negligence is an essential link in the chain of causation.” *Id.* at 704–05 (emphasis added).

Here, given AT&T’s longstanding knowledge of SIM swap vulnerabilities and attacks on its other customers, Mr. Williams’ attack was not “entirely improbable” and AT&T cannot argue that it had “no reasonable ground to anticipate” the attack. Indeed, AT&T’s negligence was an “essential link in the chain of causation.” Not only was an illegal SIM swap foreseeable by AT&T before any SIM swap attacks occurred,² after the first SIM swap attack, AT&T was *specifically put on notice* that Mr. Williams’ account was vulnerable to attack. If AT&T had put effective systems and protections in place after the first SIM swap on Mr. Williams’ account, none of the subsequent SIM swaps would have occurred. After the first SIM swap attack in May 2018, Mr. Williams informed AT&T in person and over the phone that he had valuable online accounts that made him particularly vulnerable to a SIM swap attack. Compl. ¶¶ 37–38, 46–47, 64–65. AT&T employees put a special notice in his account flagging that he was vulnerable to a SIM swap, and that there would be extra security measures (specifically, that he would not be SIM swapped unless he requested it in-person at a designated store with two passports) before his SIM card could be swapped. *Id.* ¶ 47. Based on AT&T’s promise of additional security, Mr. Williams decided not to close his account. *Id.* Yet, despite having actual notice that Mr. Williams’ account was at risk,

² SIM swap crimes have been a widespread and growing problem for years. The U.S. Federal Trade Commission (“FTC”) reported in 2016 that there were 1,038 reported SIM swap attacks per month in January 2013, which increased sharply to 2,658 per month by January 2016. Comp. ¶ 125. Further, the FTC reported that SIM swaps represented 6.3% of all identity thefts reported to the agency in January 2016, and that such thefts “involved all four of the major mobile carriers” – including AT&T. *Id.* Further, in September 2017, *over a year* before the first SIM swap attack on Mr. Williams, AT&T Vice President of Security Platforms published an article acknowledging that subscribers with “valuable accounts that are accessible online” are likely targets of SIM swaps. *Id.* ¶ 127. And, as stated above, the FTC warned mobile carriers in 2017 to adopt a multilevel approach to authenticating customers during transactions. *Id.* ¶ 126.

six other SIM swaps occurred. *Id.* ¶¶ 37–81. The SIM swaps resulted in the cumulative loss of over \$2 million and the compromise of Mr. Williams’ extremely personal data, including his home address, his and his family’s social security numbers, color-copies of their passports, their TSA numbers, password and log-in information for additional accounts, and confidential financial, business, and legal records. *Id.* ¶¶ 82–90.

AT&T should have had adequate security measures in place to guard against the highly foreseeable and likely act that hackers would actively seek to obtain the personal information of AT&T customers. The prevalence of hacking is not only highly publicized (and thus generally foreseeable) but is specifically at issue in this case given that AT&T is statutorily required to guard against hackers in order to protect its customers’ personal information. *Id.* ¶¶ 100–06. Additionally, Mr. Williams alleged that AT&T knew or should have known about the risk of SIM swap crimes, as it has been a growing problem that the FTC warned mobile carriers about well before his SIM swap. *Id.* ¶¶ 125–26, 140–45. In fact, AT&T was warned by the FTC that it should “adopt a multi-level approach to authenticating both existing and new customers and require their own employees as well as third-party retailers to use it for all transactions.” *Id.* ¶ 126. AT&T itself admitted that its customers with “valuable accounts that are accessible online” are likely targets of SIM swaps. *Id.* ¶ 127. Further, AT&T’s Vice President of Security noted that hackers were “conducting SIM swap[] attacks to seize control over victims’ phone numbers.” *Id.* ¶ 135. AT&T has also advised that “[your] phone is [your] life” and it is necessary to think about “what would a hacker want to do, where would a hacker go to get [] data, what are some of the points on [] the network that are most vulnerable, or where is the flow that is potentially going to be a leakage.” *Id.* ¶¶ 131–32.

AT&T's reliance on *Davenport v. D.M. Rental Properties, Inc.*, 718 S.E.2d 188, 190 (N.C. Ct. App. 2011), is misplaced. There, an individual described as drunk, having a bad "crack habit," delusional, and aggressive, attacked the plaintiff on the defendant landlord's property. The plaintiff sued his landlord, arguing that he was attacked because the landlord breached its duty to him by failing to install security cameras, hire security guards, install fences, or post warning signs. *Id.* The court held, however, that because of the intoxicated and irrational nature of the attacker, "the proposed safety measures would not have prevented the plaintiff's injury" and so the landlord could not be held liable. *Id.*

The facts in this case could not be more different. Here, Mr. Williams alleged that the hackers could have been stopped *but for* AT&T's failures. Specifically, Mr. Williams pled that "AT&T failed to implement sufficient data security systems and procedures and failed to supervise its own personnel, instead standing by as its employees negligently and/or purposefully helped third party hackers gain unauthorized access to his account in order to rob, extort, and threaten him and his associates." Compl. ¶ 5. Mr. Williams also alleged that "AT&T failed to put in place adequate systems and procedures to prevent the unauthorized employee access to and changes to Mr. Williams' account and related data. AT&T failed to properly hire and supervise its employees, allowing them to access Mr. Williams' sensitive and confidential account data, update his account without authorization, and give control of his account to third-party hackers." *Id.* ¶ 147.³ But for AT&T's breach of its duties⁴, Mr. Williams' data would not have been accessed by unauthorized

³ The FCC has also stated that "[t]o the extent that a carrier's failure to take reasonable precautions renders private customer information unprotected or results in disclosure of individually identifiable CPNI, . . . a violation of section 222 may have occurred." Compl. ¶ 95.

⁴ AT&T claims that Mr. Williams "own allegations indicate that these third parties would not have been deterred by anything AT&T might've done differently" but provides no citations to the Complaint supporting this statement. Mot. at 10.

individuals. *Id.* ¶ 201. Thus, unlike the attack in *Davenport*, the hackers could have been stopped had AT&T put adequate systems in place to stop unauthorized SIM swaps and/or properly hired and supervised its employees.

Given AT&T's *own admonition* to customers about the risks of SIM swaps, its claims that Mr. Williams' SIM swap was caused by unforeseeable events ring hollow. The events were foreseeable, and AT&T could have stopped the illegal SIM swaps if it had fulfilled its statutory duty. The Court should reject AT&T's arguments regarding proximate causation.

C. Mr. Williams Has Established Article III Standing.

AT&T's argument that Mr. Williams lacks standing is wrong and distorts the facts. To establish Article III standing, "[t]he plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016). Here, AT&T's contention that Mr. Williams failed to plead injury in fact is belied by the record.

At minimum, Mr. Williams alleged that hackers stole .23 bitcoin ("BTC")⁵ and \$6,500 from him, as well as color copies of his passport, social security number, TSA precheck number, and his confidential financial, business, and legal information. Compl. ¶¶ 42, 79, 84. These losses alone are enough to establish injury in fact in a standing analysis.

Mr. Williams also alleged he suffered other damages because of the SIM swaps, including that he had to shut down a business in which he had invested over \$2 million.⁶ This loss constitutes

⁵ Each BTC was worth approximately \$6,446.00 on November 5, 2018 (the day it was stolen), so hackers stole around \$1,500 from him. Compl. ¶ 42.

⁶ Contrary to AT&T's assertions, Mr. Williams provided more than a "rounded valuation" of the business as \$2 million; he alleged in detail how his investment was worth \$2 million by noting that he invested in around 500 servers to mine BTC, which cost \$2,830.00 each, paid another \$650,000 to optimize the servers and covered the cost necessary to power them. Compl.

injury in fact under North Carolina law. *See, e.g., Nat'l Fin. Partners Corp. v. Ray*, 2014 WL 5148197, at *5 (Sup. Ct. Union Cnty. Oct. 13, 2014) (noting that cross-claimants' loss of investment in a business is "injury-in-fact" that confers standing). In any event, damages analysis is not appropriate at this stage and should instead be contested during discovery. *See W. Cap. Partners, LLC v. Brookhollow, LLC*, 2007 WL 1202851, at *1 (E.D. Va. Apr. 19, 2007) (noting determination of damages was inappropriate at the motion to dismiss stage as there were factual issues surrounding it).⁷

D. Mr. Williams Is Entitled to Damages and Injunctive Relief under the Federal Communications Act.

AT&T quotes a few out-of-circuit cases to argue that Mr. Williams is not entitled to presumed damages, injunctive relief, or emotional damages under the Federal Communications Act ("FCA"). This argument fails for two reasons. First, nothing in 47 U.S.C. § 222 disallows those remedies. Second, the cases AT&T cites are non-binding precedent and inapposite. In *Conboy v. AT&T Corp.*, for example, the plaintiffs explicitly abandoned any claim for emotional distress damages. 241 F.3d 242, 250 (2d Cir. 2001). In *In re Communications Satellite Corp.*, 97 F.C.C.2d 82, 90 (1984), the Commission noted only that, damages are not presumed to follow from violations of the FCA, but that the complainant "*must allege and prove specific damages flowing from violations of the Act.*" *Id.* Similarly, in *International Telecommunications Exchange*

¶¶ 32–33, 76. Mr. Williams also alleged that he had to shut down the servers due to constantly being hacked. Thus in addition to losing his investment, he lost the ability to mine BTC (he was mining around 5–9 per month when he was forced to shut down). *Id.* ¶ 77.

⁷ Any suggestion that the court lacks jurisdiction because of a supposed paucity of damages also is ridiculous as the Complaint alleges numerous bases for subject matter jurisdiction, including federal question. *See Comp.* ¶ 15 ("This Court has jurisdiction over this matter under 28 U.S.C. § 1331 because this case arises under federal question jurisdiction under the Federal Communications Act ('FCA'). The Court has supplemental jurisdiction under 28 U.S.C. § 1367 over the state law claims because the claims are derived from a common nucleus of operative facts.").

Corp. v. MCI Telecommunications Corp., 892 F. Supp. 1520, 1545 (N.D. Ga. 1995), the court noted merely that damages are not presumed under the FCA, but that the plaintiff needed to allege actual or consequential damages from the FCA violation to recover.

Here, Mr. Williams *did* allege specific damages from AT&T's violations of the FCA, including loss of money, dissemination of his personal and sensitive information, anxiety, loss of sleep, depression, personal humiliation, mental anguish, and suffering. Compl. ¶¶ 83–84, 89, 178.

Further, this court should not follow the one out-of-circuit case (*Conway v. AT&T*) that AT&T quoted that found that emotional distress and other damages are not available under the FCA. Mr. Williams is entitled to emotional damages under his FCA claim. In its arguments, AT&T ignores that privacy injuries, and the legislation enacted to remedy them, are unique. These injuries involve fundamental interests that are not always susceptible to more traditional methods of economic quantification. Because of the unique nature of privacy injuries, laws protecting individuals' privacy rights should allow for damages in line with the uniqueness of the injury.

The Privacy Act of 1974, and caselaw interpreting it, can provide this Court with an appropriate framework in which to assess the issue of damages under the Federal Communications Act's privacy provisions. Like Section 222, Congress enacted the Privacy Act to “provide certain safeguards for an individual against an invasion of personal privacy.” *Devine v. United States*, 202 F.3d 547, 550 (2d Cir. 2000) (citation omitted). In *Bechhoefer v. Department of Justice*, 209 F.3d 57, 62 (2d Cir. 2000), *aff'd*, 312 F.3d 563 (2d Cir. 2002), this court found that the Privacy Act's protection of “personal information” extended to an individual's address and telephone number, which is similar information to Mr. Williams' CPNI and his other personal data at issue here.

In a Fifth Circuit case, *Johnson v. Department of Treasury*, 700 F.2d 971 (5th Cir. 1983), *abrogated by Doe v. Chao*, 124 S. Ct. 1204 (2004), the court had to construe the meaning of “actual

damages” under 5 U.S.C. § 552a(g)(4). Looking to the legislative intent, it found that the Privacy Act was “designed to prevent . . . the wrongful disclosure and use . . . of personal files held by the Federal government.” *Id.* at 975 (citation omitted). The court noted that “[t]he Supreme Court has indicated that the primary damage in ‘right to privacy’ cases is *mental distress*.” *Id.* at 977 (citing *Time, Inc. v. Hill*, 385 U.S. 374 (1967) (emphasis added)). The court also noted:

Obviously, mental distress is the normal and typical damage resulting from an invasion of privacy, an invasion of “our respect for the inviolability of the human personality.” *Interpreting “actual damages” to include only out-of-pocket losses would not only preclude recovery in large numbers of cases but also run counter to Congress’ intent* A federal act affording special protection to the right of privacy can hardly accomplish its purpose of protecting a personal and fundamental constitutional right if the primary damage resulting from an invasion of privacy is not recoverable under the major remedy of “actual damages” that has been provided by Congress.

Id. (citation and footnote omitted; emphasis added).

Here, this court should not choose to follow the few out-of-circuit cases AT&T cited. Instead, as intended by Congress when it enacted the legislation, Mr. Williams is entitled to presumed damages, emotional damages, and injunctive relief under the FCA.

E. Mr. Williams Alleges Reliance Under the North Carolina Unfair and Deceptive Trade Practices Act.

Pursuant to the North Carolina Unfair and Deceptive Trade Practices Act (“NCUDTPA”), Mr. Williams adequately alleged reliance on AT&T’s misrepresentations that his account would be safe.

Specifically, Mr. Williams alleged that:

- In November 2018, AT&T promised him it would add extra security to his phone, including assuring him that his SIM card would only be swapped if he entered into a

designated store with two passports. Compl. ¶ 47. Because of this representation, Mr. Williams “decided not to close his AT&T wireless account.” *Id.*

- On or around November 30, 2018, Mr. Williams was told that an AT&T employee named Steve helped an individual claiming to be Mr. Williams effectuate a SIM swap attack. *Id.* ¶ 52. The individual pretending to be Mr. Williams was able to swap Mr. Williams’ SIM despite only providing a fake driver’s license as verification of his identity, which was a direct violation of AT&T’s representations that Mr. Williams’ SIM card could not be changed absent identity verification in the form of two valid passports. *Id.*
- On December 2, 2018, AT&T employees told Mr. Williams to purchase a new iPhone to mitigate the risk of another SIM swap attack. *Id.* ¶ 57. AT&T employees also told him that there were warning messages in his account directing employees not to swap his SIM card unless he entered a designated store with two passports. *Id.* AT&T employees also advised that he was on a special list of individuals who were at high-risk for SIM swaps. *Id.* ¶ 58. Thereafter, an AT&T representative with whom Mr. Williams spoke informed him that there was no warning message in his account. *Id.* ¶ 63. No explanation was provided for this omission.
- On December 5, 2018, however, Mr. Williams asked AT&T employees if there was a warning in his account that would direct AT&T not to effectuate a SIM swap unless Mr. Williams asked in person at the designated AT&T retail store with two passports. *Id.* ¶ 64. Unlike previous times, AT&T employees confirmed there was a note in his account regarding SIM swap procedures. *Id.* Despite assurances that this note would

protect his account, Mr. Williams was attacked via SIM swap again on February 4, 2019. *Id.* ¶ 66.

Based on the foregoing, AT&T misrepresented that: (i) Mr. Williams' SIM card would be swapped only if he entered into a designated store with two passports (this was a material representation, as it was swapped *six more times* after this misrepresentation), *Id.* ¶ 47; (ii) a new iPhone would mitigate the risk of another SIM swap attack (this was a material representation, as Mr. Williams' SIM card was swapped *three more times* after this misrepresentation), *Id.* ¶ 57; (iii) warning messages were placed in his account on December 2, 2018, regarding the potential SIM swap attacks (this was a material misrepresentation as at least one time after this, AT&T employees told him there were no warning messages in his account), *Id.* ¶ 63; and (iv) when there finally was a warning message in his account, that the message would mitigate the risk of another SIM swap (this was a material representation as Mr. Williams was SIM swapped despite this warning message), *Id.* ¶ 66.

Mr. Williams alleged that he relied on these statements by purchasing a new phone and deciding not to terminate his service with AT&T. *Id.* ¶¶ 47, 57. This is enough to satisfy the pleading requirements of the NCUDTPA.

Regarding AT&T's argument on particularity, AT&T fails to note that North Carolina courts are split on whether plaintiffs must plead violation of the NCUDTPA with particularity under Rule 9(b). *See CBP Res., Inc. v. SGS Control Servs., Inc.*, 394 F. Supp. 2d 733, 739 (M.D.N.C. 2005) ("The court . . . declin[es] to extend Rule 9(b)'s coverage to claims under North Carolina's Chapter 75."); *Bussian v. DaimlerChrysler Corp.*, 411 F. Supp. 2d 614, 621 (M.D.N.C. 2006) (noting that "a higher level of specificity is not required of Plaintiff at the pleadings stage"); *FTC v. Affiliate Strategies, Inc.*, 2010 WL 11470099, at *7 (D. Kan. June 4, 2010) (applying North

Carolina law and noting that “fraud is not a necessary element of the statutory claim, North Carolina courts have found that a claim need only be pled in accordance with the state’s Rule 12(b)(6) standards.”).

However, if this Court chooses to apply 9(b) standards to Mr. Williams’ claims, he pled his NCUDTPA claim with the requisite particularity Mr. Williams alleged who (AT&T employees), what (his SIM card would only be swapped if he entered into the designated store with two passports; he should buy a new phone to mitigate his risks; there was a warning message in his account; and the warning message would mitigate the risk of SIM swaps), when (Mr. Williams provided dates of all misrepresentations and his reliance on them), where (via the phone or in the Raleigh AT&T store), and why (he relied on AT&T’s statements when he decided not to terminate his account, purchased a new iPhone, and continued service with AT&T). *Accord Madison River Mgmt. Co. v. Bus. Mgmt. Software Corp.*, 351 F. Supp. 2d 436, 447 n.6 (M.D.N.C. 2005) (“In construing Rule 9(b), courts require that a plaintiff plead the ‘time, place, and contents of the alleged fraudulent representation, as well as the identity of each person making the misrepresentation and what was obtained thereby.’”) (citation omitted); *see also U.S. ex rel. Nathan v. Takeda Pharms. N. Am., Inc.*, 707 F.3d 451, 455 (4th Cir. 2013) (“In alleging fraud or mistake, a party must state with particularity the circumstances constituting fraud or mistake.”).

In *McCauley v. Home Loan Investment Bank, F.S.B.*, 710 F.3d 551, 559 (4th Cir. 2013), the court noted that it “hesitate[s] to dismiss a complaint under Rule 9(b) if [it is] satisfied (1) that the defendant has been made aware of the particular circumstances for which [it] will have to prepare a defense at trial, and (2) that plaintiff has substantial prediscovery evidence of those facts.” In *McCauley*, the court found the plaintiff met the pleading requirements of Rule 9(b) when the plaintiff had alleged that the fraud occurred in late summer or fall 2006, where the alleged

fraud took place, what the false representations were, the name of the company that made the false representations, and that the plaintiff relied on the misrepresentations and was harmed. *Id.* Here, Mr. Williams has alleged AT&T's misrepresentations and his reliance in more detail than the plaintiff in *McCauley*.

F. Mr. Williams' Claims Are Not Barred By the Economic Loss Doctrine

AT&T incorrectly argues that Mr. Williams' negligence and negligent supervision claims are barred by the economic loss rule. Under the economic loss rule, a plaintiff cannot bring a tort action seeking to recover purely economic losses that arise out of an alleged breach of a duty created by a contractual relationship. *See* Mot. at 16 (citing *Kelly v. Ga.-Pac. LLC*, 671 F. Supp. 2d 785, 791 (E.D.N.C. 2009) ("The economic loss rule bars recovery for purely economic loss in tort when a contract, warranty, or the UCC operates to allocate risk.")). However, AT&T fails to note that this doctrine is not without limitation. In *N.C. State Ports Auth. v. Lloyd A. Fry Roofing Co.*, 240 S.E.2d 345, 351 (N.C. 1978) ("*Ports Auth.*"), *rejected by Trs. Of Rowan Tech. Coll. v. J. Hyatt Hammond Assocs., Inc.*, 313 N.D.C 230 (1985), the seminal North Carolina case establishing the economic loss doctrine, the Supreme Court of North Carolina recognized four exceptions to the rule. It held that the economic loss doctrine does not bar recovery in tort when: (1) injury or damage is to a person or property of someone other than the promisee; (2) injury or damage is to property of the promisee other than that which was the subject of the contract; (3) the promisor was charged by law, as a matter of public policy, with the duty to use care in the safeguarding of the property from harm; or (4) there was a willful injury to or conversion of the property of the promisee. *Id.* The second and third exceptions apply here.

1. Mr. Williams Sustained Injury Outside the Scope of the Privacy Policy

In the contract that Mr. Williams attached to the Complaint, AT&T's Privacy Policy, AT&T states that "Whenever you do something like buy one of our products, watch a show or download an app, information is created. Because we know your privacy is important, we have a Privacy Policy to explain how we collect, use and protect that information." Compl., Ex. A. This contract contemplates and governs the *use of specific types* Mr. Williams' private data. It specifically notes that the data it collects can be categorized into account information (such as contact and billing information), technical and usage information, location information, and TV watching information. *Id.* The Privacy Policy contemplates injury or damage from AT&T selling or utilizing *those specific categories* of Mr. Williams' data. It does not, however, address, contemplate, or govern Mr. Williams' private data that was compromised by the SIM swaps. It does not contemplate injury or damage to his finances (including the fact that thousands of dollars were stolen from his account and that he had to shut down a profitable cryptocurrency investment), and notes that special rules outside of the contract apply to his CPNI. *Id.*, Ex. A. ("Unique rules apply to CPNI."). Similarly, the Privacy Policy does not contemplate or govern what happens when AT&T's failure to protect his information causes emotional harm, suffering, personal anguish, and potential injury to Mr. Williams and his family (for example when a hacker threatened him and his daughter). *See, e.g.* Compl. ¶¶ 32–33, 42, 48, 76, 79, 84. At bottom, the injuries suffered by Mr. Williams due to AT&T's negligence and negligent supervision are outside the scope of AT&T's Privacy Policy. Accordingly, the economic loss rule does not apply.

2. AT&T is Charged by Law to Protect Mr. Williams' CPNI

The third exception to the economic loss rule also applies here because AT&T was "charged by law, as a matter of public policy, with the duty to use care in the safeguarding" of Mr.

Williams’ property from harm. *Port Auth.*, 294 N.C. at 351. For this exception, the proper inquiry is whether there is an independent legal duty, which is identifiable and distinct from the contractual duty. *Legacy Data Access, Inc. v. Cadrillion, LLC*, 889 F.3d 158, 166 (4th Cir. 2018); *Sea Side Villas II Horizontal Prop. Regime v. Single Source Roofing, Corp.*, 64 F. App’x. 367, 373 (4th Cir. 2003) (noting that a violation of a building code violates a legal duty for which a builder’s negligence is not barred by the economic loss rule).

Here, the FCA imposes on AT&T an independent legal duty, outside of its contractual duty, to keep Mr. Williams’ CPNI safe. AT&T is a common carrier governed by the FCA, and pursuant to the FCA, the FCC has developed comprehensive rules concerning AT&T’s obligations under its duty to protect customers’ CPNI.⁸ Compl. ¶ 104. These include rules “designed to ensure that telecommunications carriers establish effective safeguards to protect against unauthorized use or disclosure of CPNI.” *Id.* Under the FCC’s rules, AT&T must implement a system by which the status of a customer’s CPNI approval can be clearly established prior to the use of CPNI.” *Id.* ¶ 105. The FCC also requires AT&T to “design their customer service records in such a way that the status of a customer’s CPNI approval can be clearly established.” *Id.* The FCC’s rules also

⁸ Courts in North Carolina and the Fourth Circuit have noted that the third exception applies to common carriers, because they are charged by law with the duty to use care. *In re New Bern Riverfront Dev., LLC*, 2011 WL 5902621, at *5 (Bankr. E.D.N.C. May 24, 2011); *Legacy Data Access*, 889 F.3d at 165 (“[T]he economic loss rule does not prohibit tort claims against a defendant who, in addition to and independent of his contractual duty, is ‘charged by law, as a matter of public policy, with the duty to use care in the safeguarding of the property . . . **as in the case of a common carrier**’”) (emphasis added); *Hatteras/Cabo Yachts, LLC v. M/Y EPIC*, 2019 WL 5792863, at *3 (E.D.N.C. Nov. 6, 2019) (noting economic loss doctrine does not apply when “the promisor being charged by law, as a matter of public policy, with the duty to use care in the safeguarding of the property from harm, **as in the case of a common carrier**”) (emphasis added) (quotation omitted).

further “require carriers to maintain records that track access to customer CPNI records.” *Id.* The FCC has “[made] clear that carriers’ existing statutory obligations to protect their customers’ CPNI include[s] a requirement that carriers take reasonable steps, which may include encryption, to protect their CPNI databases from hackers and other unauthorized attempts by third parties to access CPNI.” *Id.* ¶ 112. The FCC has stated that “[t]o the extent that a carrier’s failure to take reasonable precautions renders private customer information unprotected or results in disclosure of individually identifiable CPNI, . . . a violation of section 222 may have occurred.” *Id.* ¶ 95.

Consistent with these statutory and regulatory statutory obligations, AT&T was subject to an FCC enforcement action in 2015 and paid a \$25 million civil penalty for nearly identical failures to protect its customers’ sensitive account data. *Id.* ¶ 140. The FCC concluded that AT&T’s “failure to reasonably secure customers’ proprietary information violates a carrier’s statutory duty under the Communications Act to protect that information, and also constitutes an unjust and unreasonable practice in violation of the Act.” *Id.* ¶ 141. The FCC stressed that the FCA is intended to “ensure that consumers can trust that carriers have taken appropriate steps to ensure that unauthorized persons are not accessing, viewing or misusing their personal information.” *Id.* ¶ 142. It also stressed its expectation that “telecommunications carriers such as AT&T . . . take ‘every reasonable precaution’ to protect their customers’ data[.]” *Id.* As a condition of its stipulated Consent Decree, AT&T agreed to develop and implement a compliance plan to ensure appropriate safeguards to protect consumers against similar breaches by improving its privacy and data security practices. *Id.* ¶ 143. These legal duties create an exception to the economic loss doctrine.

G. None of the Exceptions to the North Carolina Anti-Hacking Statute Apply Here.

AT&T incorrectly interprets the exception to the Anti-Hacking Statute (N.C. Gen. State Section 1-539.2A) (also known as the Computer Trespass Statute). The language of the exception is as follows:

This Article does not apply to or prohibit:

- (1) Any terms or conditions in a contract or license related to a computer, computer network, software, computer system, database, or telecommunication device; or
- (2) Any software or hardware designed to allow a computer, computer network, software, computer system, database, information, or telecommunication service to operate in the ordinary course of a lawful business or that is designed to allow an owner or authorized holder of information to protect data, information, or rights in it.

N.C. Gen. Stat. 14-453.1.

Mr. Williams alleged that AT&T, through its employees, used a computer or computer network with intent to disable and halt data from Mr. Williams' mobile device. Compl. ¶¶ 37–81, 224. Despite his well-pled allegations, AT&T makes a blanket statement that “[t]his telecommunications exception defeats Plaintiff’s claims.” Mot. at 18. Although there is virtually no case law interpreting the foregoing exception, it simply strains credulity to suggest that it was meant to protect unauthorized SIM swaps. This is because “[s]tatutory rules of construction require the Court to consider the language used in the statute, the mischiefs sought to be avoided, and the remedies intended to be applied.” *Appeal of Martin*, 209 S.E.2d 766, 775 (N.C. 1974). Moreover, these canons of interpretation also require that a statute be interpreted “so as to avoid an absurd consequence.” *Id.* Applying these principles to the exceptions above, a far more plausible construction emerges. The language of the exception prohibits parties from using the statute to sue companies/individuals that have either user agreements or licenses, or software and

hardware mechanisms, that could potentially violate the statute in the *normal course of business*. For example, if a software provider provides a mechanism in its software to temporarily halt private data of users (i.e. Gmail halts a user's email data until a password is provided), then these exceptions protect Google/Gmail from being sued for violating the statute. But the exception was not meant to be applied as a get-out-of-jail-free card for companies engaged in negligent and criminal conduct.

AT&T's rejoinder simply is wrong and distorts Mr. Williams' pleadings and the plain text of the statute. Mr. Williams alleged that AT&T, through its employees, violated the statute. He did not allege that terms or conditions in AT&T's contract or license violated the statute (N.C. Gen. Stat. 14-453.1 (1)), nor did he allege that software or hardware that was designed to allow AT&T to operate in the ordinary course of business violated the statute (N.C. Gen. Stat. 14-453.1 (2)). Instead, he alleged that AT&T's employees intended to disable and halt data to Mr. Williams' mobile device by conducting the unauthorized SIM swaps (and they were successful, as his phone lost service and he no longer had data). Comp. ¶¶ 37–81.

AT&T further claims that Mr. Williams made a conclusory allegation that AT&T employees made copies of Mr. Williams' confidential data. Again, it ignores the rest of the Complaint to make this claim. Importantly, the text of the statute states “it is unlawful for any person to use a computer or computer network without authority and with the intent to. . . [m]ake or ***cause to be made an unauthorized copy***, in any form, including, but not limited to, any printed or electronic form of computer data, computer programs, or computer software residing in, communicated by, or produced by a computer or computer network.” N.C. Gen. State Section 14-458(a)(5) (emphasis added).

Mr. Williams alleged that AT&T, through its employees, made or caused to be made, copies of Mr. Williams' confidential data by conducting a SIM swap. AT&T cannot allege that copies of Mr. Williams' confidential data were not made, since Mr. Williams pled that hackers used his confidential data to threaten him. *See, e.g.* Compl. ¶ 48. Contrary to AT&T's assertions, in his complaint, Mr. Williams pled specific instances where copies were made of his data due to AT&T's actions.

Accordingly, his claim under N.C. Gen. State Section 1-539.2A should not be dismissed.

H. Mr. Williams' CFAA Claim is Adequately Pled

Under the CFAA, loss is defined as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11). These nine types of loss are examples, not limitations on what qualifies as "loss" under the CFAA. *Ticketmaster L.L.C. v. Prestige Entm't W., Inc.*, 315 F. Supp. 3d 1147, 1173-74 (C.D. Cal. 2018). To prevail on a CFAA claim, a plaintiff must show "loss to 1 or more persons during any 1-year period . . . aggregating at least \$5,000 in value." 18 U.S.C. § 1030(c)(4)(A)(i)(I). That showing is met here.

AT&T's claims that Mr. Williams did not adequately plead qualifying loss in the complaint and that loss is primarily "the remedial costs of investigating a computer for damage, remedying damage done, and costs incurred while the computer is inoperable," Mot. at 21–22. This argument fails for two reasons.

First, all the cases Defendant cites are inconsistent with how the Fourth Circuit defines loss. Fourth Circuit and North Carolina courts look to the full text of the statute when defining

loss. *See, e.g., Tech Sys., Inc. v. Pyles*, 630 F. App'x 184, 186 (4th Cir. 2015) (finding a reasonable jury could have found a CFAA violation when part of the loss was lost working hours from unproductive employees due to a lack of access to the plaintiff's critical systems, and which ended up costing the plaintiff a substantial sum of money); *A.V. ex rel. Vanderhye v. iParadigms, LLC*, 562 F.3d 630, 646 (4th Cir. 2009) (finding consequential damages constituted loss under the CFAA, denying defendant's motion to dismiss CFAA claims and noting that loss included "revenue lost, costs incurred, and other consequential damages incurred"); *Tech. Partners, Inc. v. Papaioannou*, 2015 WL 9304562, at *1 (W.D.N.C. Dec. 21, 2015).

Second, contrary to AT&T's assertions, Mr. Williams pled more than a "formulaic recitation" of CFAA elements and met his pleading burden. Mot. at 20. Specifically, he pled that he lost over \$2 million because of money stolen from his bank account, stolen cryptocurrency, lost investment, and lost profits. Compl. ¶¶ 32–34, 42–43, 76–77, 79. He also pled that after each SIM swap, he would attempt to figure out what had happened, what data and accounts had been damaged, and how to mitigate those damages. *Id.* ¶ 87. This investigation included forcing Mr. Williams to fly back home from a vacation on at least one occasion to try and figure out what was going on. *Id.* ¶ 70. He further pled that he bought a new iPhone and switched to a different carrier in response to AT&T's CFAA violations. *Id.* ¶¶ 57, 80–81. Mr. Williams also pled he has suffered from anxiety, loss of sleep, and extreme depression as a result of the SIM swaps. *Id.* ¶ 89. Finally, he pled that he has spent over \$5,000 investigating what happened. *Id.* ¶ 235.

Nothing more is required at this stage, as courts have found pleading with far fewer details to be adequate. *See, e.g., Sageworks, Inc. v. Creatore*, 2017 WL 633359, at *2 (E.D.N.C. Feb. 15, 2017) (denying defendants' motion to dismiss where all that was alleged in plaintiff's claim for violation of the CFAA was "[a]s a result of Creatore's activities, Sageworks has suffered damages

in excess of \$5,000.”); *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 201 n.1 (4th Cir. 2012) (noting that the plaintiff sufficiently pled its losses when “WEC allege[d] that its aggregate losses as a result of Appellees' conduct were ‘at least \$5,000 in value’ during a one-year period, which satisfies § 1030(c)(4)(A)(i)(I).”).

The motion to dismiss the CFAA claim should therefore be denied. To the extent the Court concludes Mr. Williams has not pled loss under the CFAA, Mr. Williams respectfully requests that leave to amend should be granted to plead loss in more detail.

I. Mr. Williams’ Prayer for Punitive Damages Should Not Be Stricken

Whether AT&T is subject to punitive damages should not be resolved at the motion to dismiss stage because it “is primarily [a] factual [question.]” *Cent. Wesleyan Coll. v. W.R. Grace & Co.*, 6 F.3d 177, 184 (4th Cir. 1993). Thus, given the factual nature of the inquiry, punitive damages may only be barred at the motion to dismiss stage where they are unavailable as a matter of law. *See Newton v. Standard Fire Ins. Co.*, 291 N.C. 105, 111 (1976) (“[w]hether the facts stated in the pleadings are sufficient to bring the case within the rule allowing punitive damages is a question of law, although the determination whether punitive damages will be allowed and the amount to be allowed, if any, rests in the sound discretion of the jury.” (internal citations omitted)); *see also Sec. Credit Corp. v. Mid/East Acceptance Corp. of N.C., Inc.*, 2012 WL 1337400, at *6 (N.C. Ct. App. Apr. 17, 2012)(“[W]e hold that [the] claim for punitive damages is sufficient to withstand a 12(b)(6) motion to dismiss . . . the allegations . . . support a finding that defendants’ involvement was activated by a long history of personal ill will [and] show that defendants acted purposely, knowing that their actions would result in not only emotional and mental distress but also financial distress in having to defend the criminal and civil lawsuits filed against them.”).

Mr. Williams has adequately pled enough facts to establish his claim for punitive damages. Under North Carolina law, punitive damages may be awarded against a corporation “where the officers, directors, or managers of a corporation participated in or condoned the conduct constituting the aggravating factor giving rise to punitive damages.” North Carolina General Statute Article (“N.C.G.S.A.”) § 1D-15(c); *see also Wilkins v. Denamerica Corp.*, 2001 WL 1019698, at *3 (W.D.N.C. May 5, 2001) (To impose punitive damages on a corporation, a plaintiff must show that the illegal actions of an employee were ratified or approved by the manager); *Everhart v. O’Charley’s Inc.*, 683 S.E.2d 728, 738 (N.C. Ct. App. 2009) (noting that manager, in the context of the statutory definition of punitive damages is someone “who ‘conducts, directs, or supervises something.’”) (citation omitted). The aggravating factors required would be either (1) fraud; (2) malice; (3) willful or wanton conduct.” N.C.G.S.A. § 1D-15(a). Willful and wanton conduct is defined as “the conscious and intentional disregard of and indifference to the rights and safety of others, which the defendant knows or should know is reasonably likely to result in injury, damage, or other harm.” *Id.* § 1D-5(7).

Everhart v. O’Charley’s Inc. is instructive here. There, the court found that an employee who condoned or participated in willful and wanton conduct could be considered a “manager” for purposes of holding the corporation liable for punitive damages, if the employee was following company policy.⁹ 683 S.E.2d at 738. Importantly, the court noted that the necessary relationship between the defendant’s aggravating conduct and the plaintiff’s injuries was not that the willful and wonton conduct *caused* the injury, but only that the “plaintiff demonstrate[s] a ‘connection

⁹ The court found that following the policy could be considered willful and wanton conduct because a reasonable jury could find it “recklessly disregard[ed] customers’ safety and well-being in order to begin the process of protecting [the corporation] against potential litigation.” *Id.*

between the [aggravating conduct] and plaintiff[’s] alleged harm.” *Id.* at 738–39 (quotation omitted).

Mr. Williams has alleged both cause and connection between actions of AT&T’s directors, officers, and managers, and Mr. Williams’ injuries. In great detail, Mr. Williams pled the multiple times he was SIM swapped, including that he informed AT&T employees that he had been a victim of hacking to his mobile account and that subsequently AT&T employees promised to provide him with additional protection to prevent such fraud in the future. Compl. ¶¶ 37–38, 47, 51–52, 57–58, 62–64, 71. Further, Mr. Williams pled that AT&T was under both a statutory obligation and a duty imposed by the FCC in the Consent Decree to protect the personal information of its customers against fraud. *Id.* ¶¶ 141–44. AT&T was aware that its employees could bypass protections, and yet failed to implement a system to protect against this eventuality. *Id.* ¶¶ 146–60. In fact, AT&T’s Vice President knew that SIM swap thieves were constantly changing their tactics, and he promised that AT&T would continually enhance its safety measures in response. *Id.* ¶ 127, n.46 (citing Brian Rexroad, “*Secure Your Number to Reduce SIM Swap Scams*,” AT&T’s Cyber Aware (Sept. 2017), *available at* https://about.att.com/pages/cyberaware/ni/blog/sim_swap). AT&T and its managers, officers, and directors, including its Vice President Brian Rexroad, acted willfully and wantonly by consciously disregarding these obligations by failing to supervise its employees and permitting a system to exist where employees could readily bypass account protections. *Id.* ¶¶ 146–60, 192–220.

Construing the allegations of the Complaint in the light most favorable to Mr. Williams, the allegations show that AT&T, through its managers, officers, and directors, acted with fraud, malice and willful and wonton disregard of Mr. Williams’ rights in violating its statutory duties under Section 222(a) of the FCA and in its actions specific to Mr. Williams. Whether it was managers

in the AT&T store who SIM swapped or approved an employee to SIM swap Mr. Williams' SIM card¹⁰, or high-level executives who noted the dangers of SIM swapping, yet failed to implement systems that would protect Mr. Williams from illegal SIM swaps, Mr. Williams has alleged a connection between the wanton and willful conduct of officers, directors, or managers of AT&T and his injury. Accordingly, the claim for punitive damages should not be dismissed.

III. CONCLUSION

For the foregoing reasons, the Court should deny AT&T's Motion to Dismiss.

¹⁰ The multiple employees who SIM swapped Mr. Williams' phone illegally may be managers, which is a factual issue that should be explored in discovery.

/s/ Christopher N. LaVigne
Christopher N. LaVigne
clavigne@piercebainbridge.com
Sarah Baugh
sbaugh@piercebainbridge.com
**PIERCE BAINBRIDGE BECK
PRICE & HECHT LLP**
277 Park Avenue, 45th Floor
New York, NY 100172
Telephone: (212) 484-9866
Facsimile: (646) 968-4125

Dwayne D. Sam
dsam@piercebainbridge.com
**PIERCE BAINBRIDGE BECK
PRICE & HECHT LLP**
601 Pennsylvania Avenue NW
South Tower, Suite 700
Washington, DC 20004
Telephone: (202) 843-8342
Facsimile: (202) 899-5666

Counsel for Plaintiff Jason Williams

/s/ Terence S. Reynolds
Terence S. Reynolds
treynolds@shumaker.com
Lucas D. Garber
lgarber@shumaker.com
SHUMAKER LOOP & KENDRICK LLP
101 South Tyron Street
Suite 2200
Charlotte, North Carolina 28280
Telephone: (704) 375-0057
Facsimile: (704) 332-1197

*Local Civil Rule 83.1(d) Counsel for Plaintiff
Jason Williams*

CERTIFICATE OF SERVICE

I hereby certify that on this date, February 3, 2020, I caused the foregoing document to be filed and served on all counsel of record by operation of the CM/ECF system for the United States District Court for the Eastern District of North Carolina.

Dated: February 3, 2020

/s/ Terence S. Reynolds
Terence S. Reynolds
SHUMAKER LOOP & KENDRICK LLP
101 South Tyron Street
Suite 2200
Charlotte, North Carolina 28280
Telephone: (704) 375-0057
Facsimile: (704) 332-1197
treynolds@shumaker.com
State Bar No. 49848

*Local Civil Rule 83.1(d) Counsel for Plaintiff
Jason Williams*